UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/942,994	08/31/2001	Takuya Morishita	Q66052	9297

7590 08/26/2005

SUGHRUE, MION, ZINN, MACPEAK & SEAS
2100 Pennsylvania Avenue, N.W.
Washington, DC 20037

EXAMINER	
HA, LEYNNA A	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 08/26/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/942,994	MORISHITA, TAKUYA	
	Examiner	Art Unit	
	LEYNNA T. HA	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *8/31/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-16 has been re-examined and claims 17-19 are new claims. Claims 1-19 are pending.

2. This is a Final rejection.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Regarding claims 1-5 and 17, the word "means" is preceded by the word(s) "for performing" in an attempt to use a "means" clause to recite a claim element as a means for performing a specified function. However, since no function is specified by the word(s) preceding "means," it is impossible to determine the equivalents of the element, as required by 35 U.S.C. 112, sixth paragraph. See *Ex parte Klumb*, 159 USPQ 694 (Bd. App. 1967).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claim 18 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 18 is directed to a system for decrypting an encrypted computer program. The examiner asserts that the collection of information does not fall within the statutory classes listed in 35 USC 101. Thus, while the claimed invention may be labeled as a system that performs decryption it is in fact functional descriptive material (i.e., computer program). Claim 18 is rejected as being directed to a functional descriptive material.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1-4, 6-9, 11-14, and 16 are rejected under 35 U.S.C. 102(e) as being anticipated by Krishnan, et al. (US 6,405,316).

As per claim 1:

Krishnan, et al. discloses a system for decrypting an encrypted computer program, comprising:

means for generating a first cipher key from at least one first block of the encrypted computer program; **(col.12, lines 23-24 and 54-55 and col.16, lines 30-31)**

means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key; **(col.13, lines 45-47 and col.16, lines 40-47)**

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks **(col.3,**

lines 10-12), a second cipher key is generated from a current block and a next block is decrypted with the second cipher key. **(col.16, lines 57-63 and col.17, lines 3-6)**

As per claim 2: See col.13, line 8; discussing wherein said at least one a first block is not encrypted.

As per claim 3: See col.3, lines 8-11 and col.16, line 30-31; discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 4: See col.3, lines 8-11 and col.16, line 57-58; discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 6:

Krishnan discloses a method for decrypting an encrypted computer program, comprising the steps of:

generating a first cipher key from at least one first block of the encrypted computer program; **(col.12, lines 23-24 and 54-55 and col.16, lines 30-31)**

performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; **(col.13, lines 45-47 and col.16, lines 40-47)**

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a second cipher key is generated **(col.3, lines 10-12)** from a current block

and a next block is decrypted with the second cipher key. **(col.16, lines 57-63 and col.17, lines 3-6)**

As per claim 7: See col.13, line 8; discussing said at least one first block is not encrypted.

As per claim 8: See col.3, lines 8-11 and col.16, line 30-31; discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 9: See col.3, lines 8-11 and col.16, line 57-58; discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 11:

Krishnan discloses a computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, said method comprising the steps of:

generating a first cipher key from at least one first block of the encrypted computer program; **(col.12, lines 23-24 and 54-55 and col.16, lines 30-31)**

performing a first decryption of a plurality of second blocks of the encrypted computer program with said first cipher key; and **(col.13, lines 45-47 and col.16, lines 40-47)**

means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks, a

second cipher key is generated **(col.3, lines 10-12)** from a current block and a next block is decrypted with the second cipher key. **(col.16, lines 57-63 and col.17, lines 3-6)**

As per claim 12: See col.13, line 8; discussing said at least one block is not encrypted.

As per claim 13: See col.3, lines 8-11 and col.16, line 30-31; discussing plurality of second blocks are encrypted at least with said first cipher key prior being decrypted.

As per claim 14: See col.3, lines 8-11 and col.16, line 57-58; discussing at least one of said plurality of second blocks is encrypted with said second cipher key prior being decrypted.

As per claim 16:

Krishnan discusses data structure embodied on a computer-readable medium comprising:

a non-encrypted block; and **(col.13, line 8;)**

a plurality of encrypted blocks; **(col.12, line 18 and col.16, line 40)**

wherein said plurality of encrypted blocks are encrypted with a cipher key generated from said non-encrypted block, and **(col.13, lines 21-22 and col.12, lines 54-56)**

wherein for each of said plurality of second blocks **(col.3, lines 10-12)**, a next block is encrypted with a cipher key which is generated from a current block. **(col.16, lines 57-63 and col.17, lines 3-6)**

As per claim 17:

Krishnan discloses a system for decrypting an encrypted computer program, comprising:

means for generating cipher keys for a plurality of blocks, and **(col.12, lines 23-24 and 54-55 and col.16, lines 30-31)**

means for performing a decryption of the plurality of blocks, **(col.13, lines 45-47 and col.16, lines 40-47)**

wherein for each of said plurality of second blocks **(col.3, lines 10-12)**, a cipher key is generated from a current block and a next block is decrypted said cipher key. **(col.16, lines 57-63 and col.17, lines 3-6)**

As per claim 18:

Krishnan discusses a system for decrypting an encrypted computer program, comprising a step of:

performing a decryption of the plurality of blocks, **(col.13, lines 45-47 and col.16, lines 40-47)**

wherein for each of said plurality of second blocks **(col.3, lines 10-12)**, a cipher key is generated from a current block and a next block is decrypted said cipher key. **(col.16, lines 57-63 and col.17, lines 3-6)**

As per claim 19:

Krishnan discusses a computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, comprising a step of:

performing a decryption of the plurality of blocks, **(col.13, lines 45-47 and col.16, lines 40-47)**

wherein for each of said plurality of second blocks **(col.3, lines 10-12)**, a cipher key is generated from a current block and a next block is decrypted with said cipher key. **(col.16, lines 57-63 and col.17, lines 3-6)**

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 5, 10, and 15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan, et al. (US 6,405,316) in further view of Lotspiech, Et Al. (US 6,118,873).

As per claim 5:

Krishnan, et al. discloses a system for decrypting an encrypted computer program, comprising means for generating a first cipher key

from at least one first block of the encrypted computer program (col.12, lines 23-24 and 54-55 and col.16, lines 30-31), means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key (col.13, lines 45-47 and col.16, lines 40-47), and means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks (col.3, lines 10-12), a second cipher key is generated from a current block and a next block is decrypted with the second cipher key (col.16, lines 57-63 and col.17, lines 3-6). Although, Krishnan discusses determining the blocks of data that will be encrypted (col.12, lines 17-18) and the system as set forth in claim 1, but fails to discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of

second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Krishnan with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program would determine whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

As per claim 10:

Krishnan, et al. discloses a system for decrypting an encrypted computer program, comprising means for generating a first cipher key from at least one first block of the encrypted computer program (col.12, lines 23-24 and 54-55 and col.16, lines 30-31), means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key (col.13, lines 45-47 and col.16, lines 40-47), and means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks (col.3, lines 10-12), a second cipher key is generated from a current block and a

next block is decrypted with the second cipher key (col.16, lines 57-63 and col.17, lines 3-6). Although, Krishnan discusses determining the blocks of data that will be encrypted (col.12, lines 17-18) and the system as set forth in claim 1, but fails to discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Krishnan with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech

because by analyzing the program would determine whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

As per claim 15:

Krishnan, et al. discloses a system for decrypting an encrypted computer program, comprising means for generating a first cipher key from at least one first block of the encrypted computer program (col.12, lines 23-24 and 54-55 and col.16, lines 30-31), means for performing a first decryption a plurality of second blocks of the encrypted computer program with said first cipher key (col.13, lines 45-47 and col.16, lines 40-47), and means for performing a second decryption of the plurality of second blocks, wherein for each of said plurality of second blocks (col.3, lines 10-12), a second cipher key is generated from a current block and a next block is decrypted with the second cipher key (col.16, lines 57-63 and col.17, lines 3-6). Although, Krishnan discusses determining the blocks of data that will be encrypted (col.12, lines 17-18) and the system as set forth in claim 1, but fails to discuss in details the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed.

Lotspiech, et al., discloses a system for encrypting broadcast programs running on plural devices and to determine whether the devices running the programs have been compromised. Lotspiech discusses means for determining whether or not the encrypted computer program is analyzed to determine whether any devices have been compromised **(col.6, lines 52-54 and col.8, lines 16-35)** and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed **(col.7, lines 26-31 and col.8, lines 24-26)**.

It would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the teachings of Krishnan with the means for determining whether or not the encrypted computer program is analyzed and means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if the encrypted computer program is determined to be analyzed as taught by Lotspiech because by analyzing the program would determine whether any devices have been compromised and to decrypt the dummy blocks rather than the plurality of second blocks so that it prevents the unwanted and unauthorized user or device from obtaining the real key thereby to the actual program.

Response to Arguments

7. Applicant's arguments with respect to claims 1-19 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

8. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LEYNNA T. HA whose telephone number is (571) 272-3851. The examiner can normally be reached on Monday - Thursday (7:00 - 5:00PM).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

LHa

Primary Examiner
Art Unit 2135